



Unmasking Anonymous: An Eyewitness Account of a Hacktivist Attack

Tal Be'ery
Web Security Research Team Leader
Imperva



Agenda

- Anonymous Overview and Background
- How They Attack: Anatomy of an Anonymous Attack
 - + Recruiting and Communications
 - + Reconnaissance and Application Attack
 - + DDoS
- Mitigations
 - + What's hot - Mitigation Tools
 - + What's not - Non-Mitigations Tools

Speaker Bio – Tal Be'ery

- Web Security Research Team Leader at Imperva
- Holds MSc & BSc degree in CS/EE from TAU
- Decade of experience in the IS domain
- Facebook "white hat"
- Speaker at Industry Events
 - RSA, blackhat, AusCERT
- CISSP



Hacktivism - definition

"Hacktivism -
a portmanteau of hack and activism."



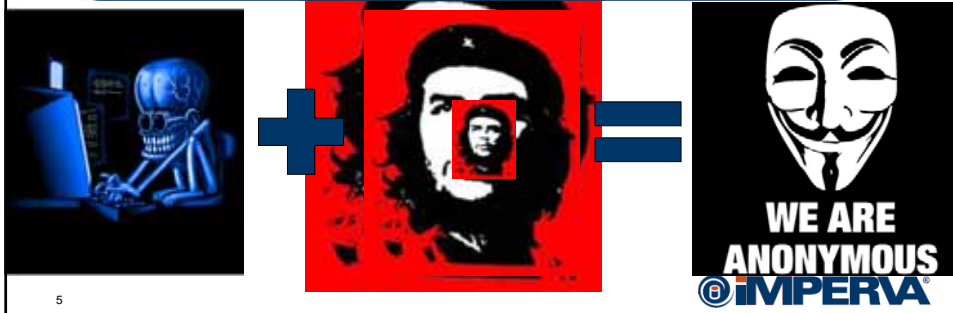
What/Who is Anonymous?

"...the first Internet-based superconsciousness."

—Chris Landers. *Baltimore City Paper*, April 2, 2008

"Anonymous is an umbrella for anyone to hack anything for any reason."

—*New York Times*, 27 Feb 2012



What/Who is Anonymous?

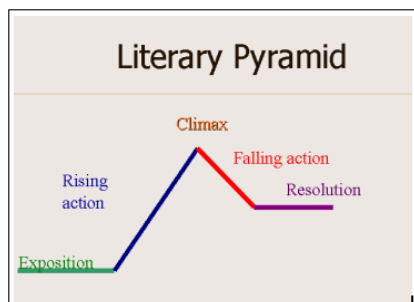
- One thing is for sure - they are hackers!



© IMPERVA®

6

The Plot



- Attack took place in 2011 over a 25 day period.
- Anonymous was on a deadline to breach and disrupt a website, a proactive attempt at hacktivism.
- The website was mostly informational but contained data and enabled some commerce.
- The attack was not successful.

7



On the Offense



+ Skilled hackers –

- Small group , few individuals per campaign
- have genuine hacking experience and are quite savvy.



+ Nontechnical –

- can be quite large, ranging from a few dozens to a few hundred volunteers.
- Directed by the skilled hackers
- Providing the needed “muscles” to conduct DDoS attacks.

8



On the Defense



- Deployment line was network firewall and IDS, web application firewall (WAF), web servers and anti-virus.
- Imperva WAF
 - + SecureSphere WAF version 8.5 inline, high availability
 - + ThreatRadar reputation services
- Unnamed network firewall and IDS
- Unnamed anti-virus

9



How They Attack: The Anonymous Attack Anatomy



10

for more: http://www.imperva.com/docs/HII_The_Anatomy_of_an_Anonymous_Attack.pdf



1

Recruiting and Communications



Step 1A: An "Inspirational" Video



12



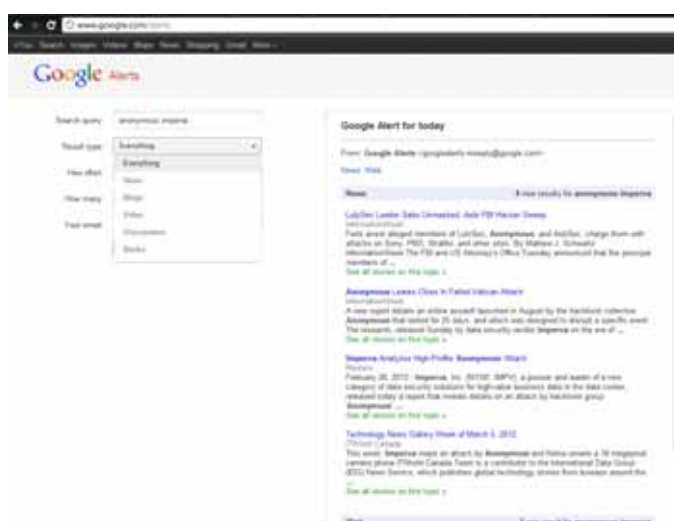
Step 1B: Social Media Helps Recruit



13



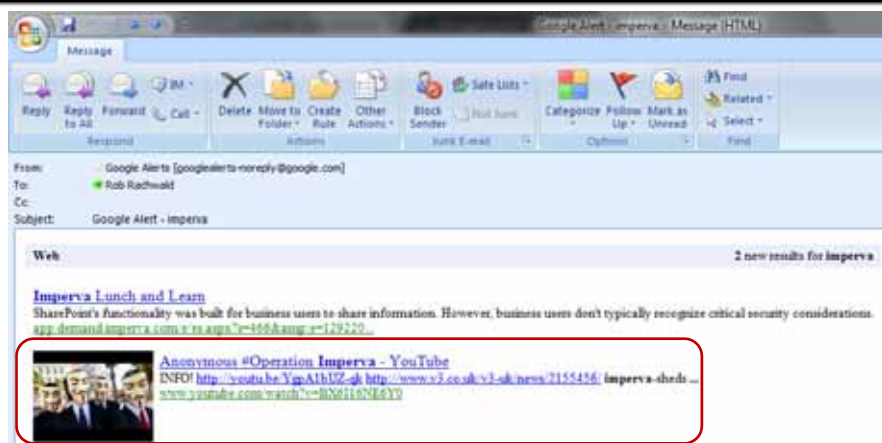
Setting Up An Early Warning System



14



Example



15



2

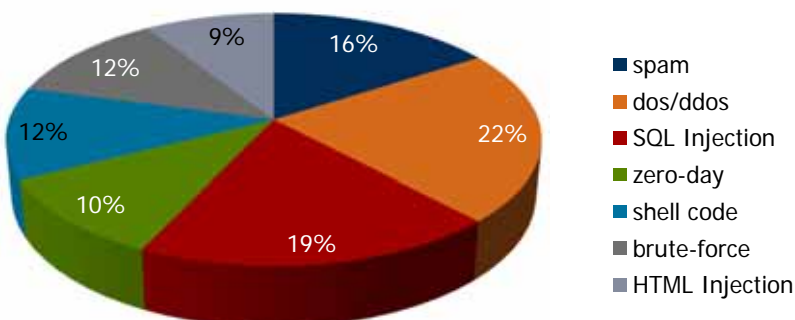
Recon and Application Attack

"Avoid strength, attack weakness: Striking where the enemy is most vulnerable."
—Sun Tzu



Anonymous' Attacks Mimic For-Profit Hackers

Hacker Forum Discussion Topics



Source: Imperva. Covers July 2010 -July 2011 across 600,000 discussions

17

© 2012 Imperva, Inc. All rights reserved.



Step 2A: Finding Vulnerabilities

- Tool #1: Vulnerability Scanners
- Purpose: Rapidly find application vulnerabilities.
- Cost: \$0-\$1000 per license.
- The specific tools:
 - + Acunetix (named a "Visionary" in a Gartner 2011 MQ)
 - + Nikto (open source)



```
GET /php?root=script=script=alert('Vulnerable!')&script= HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.2; en-US; rv:1.9.0.3) Gecko/2008092417 Firefox/3.0
X-Akamai-CONFIG-LOG-DETAIL: true
TE: chunked;q=1.0
Connection: TE
Accept-Encoding: gzip
```



```
GET /php?root=script=script=alert('Vulnerable!')&script= HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.2; en-US; rv:1.9.0.3) Gecko/2008092417 Firefox/3.0
X-Akamai-CONFIG-LOG-DETAIL: true
TE: chunked;q=1.0
Connection: TE
Accept-Encoding: gzip
```

18



Step 2B: Exploiting Vulnerabilities

- Tool #2: Havij
- Purpose:
 - + Automated SQL injection and data harvesting tool.
- Developed in Iran



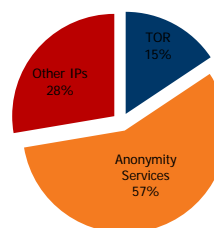
```
GET /php?id=106147073' and ascii(substring((SELECT distinct table_name FROM information_sche
ma.tables Where table_schema=0x202020 limit 0,1),2,1))=56 and 'x'='x HTTP/1.1
Host: [redacted]
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727) Havij
Connection: Close
```

19

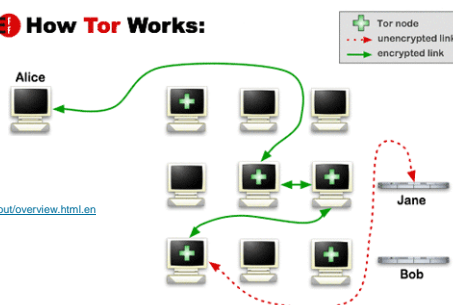


Protecting true Identity

- Hacker protect their identity
- By using
 - + TOR
 - + Other anonymity services
 - Anonymous proxies
 - Private VPN services
 - Hacked servers



How Tor Works:



20



Why hackers prefer using exploits over DDoS?

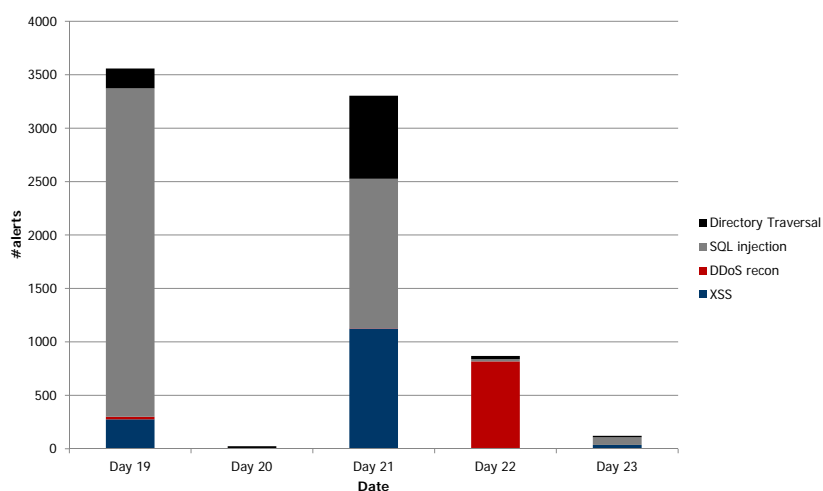
	Exploits	DDoS
Damage	Inflict damage to all aspects of data security – availability	Only data availability
Cost		Hundreds, thousands..
Effect	Long lasting	Only during the attack

Exploits are the hackers first choice
DDoS is just a last resort

21



Vulnerabilities of Interest



22



Lulzsec hack Analysis #1- PBS

- SQL injection
- Exploited by Havij
- Defacement
- Administrative Data leakage

Havij 1.14 Pro by e3dm0v3

Date: 5/24/2011 10:07:18 AM
 DB Detection: MySQL 5.0 (Auto Detected)
 Method: SST
 Type: Blog (Auto Detected)
 Data Base: mysql
 Table: user
 Total Rows: 290

Host	User	Password
10.10.10.10	admin	123456789



23



Lulzsec hack Analysis #2- Militarysingles.com

- Executable file upload
- PII of 170K users leaked

www.militarysingles.com/esvonyfiles/small/7C=M;O=D			
Picture0003_1.JPG	26-Mar-2012 20:32	8.3K	
132084_1.jpg	26-Mar-2012 20:32	7.5K	
132084.jpg	26-Mar-2012 20:32	3.3K	
1.jpg	26-Mar-2012 19:54	4.0K	



24



Mitigation: AppSec 101

Dork Yourself

Blacklisting

WAF

WAF + VA

Stop Automated
Attacks

Code Fixing

25



3

DDoS - the last refuge of a hacker



Hacking Tools

- Low-Orbit Ion Canon (LOIC)
- Purpose - DDoS
- Windows desktop application, coded in C#
- UDP/TCP/HTTP flooding



LOIC Facts

- LOIC downloads
 - + 2011: 380K
 - + 2012 (through April 22): 380K
 - + Jan 2012 (megaupload takedown) =83% of 2011's downloads!

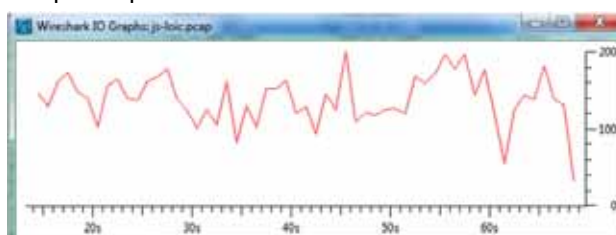


For more: <http://blog.imperva.com/2012/05/loicversary.html>



Javascript/Mobile/VM/JS LOIC

- DaaS – DoS as a Service
- Easy to participate – no download
 - + just point your browser to the JS-Loic page
- Application layer attacks
- Effective
 - + Iterates up to 200 requests per second
- Cross platform
 - + mobile device
 - + Linux/Mac/PC



29

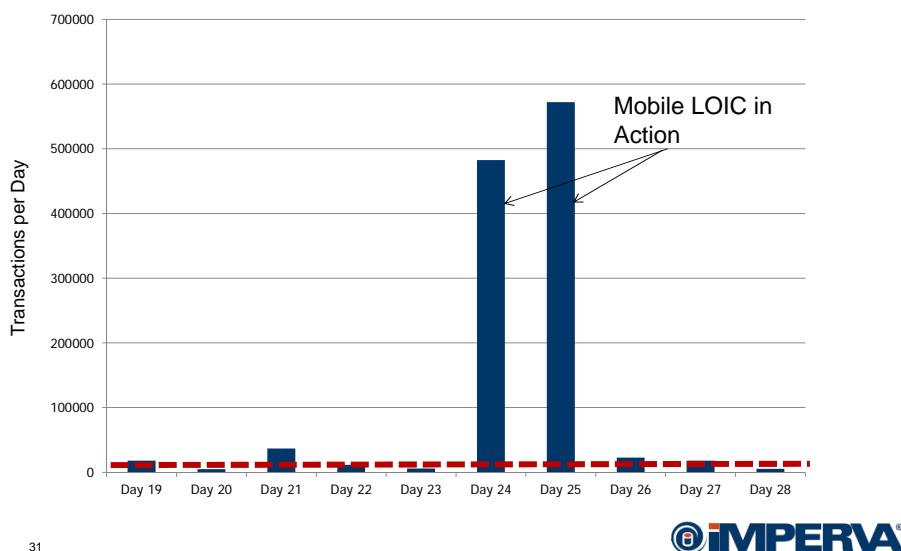
JS LOIC - Attack Characteristics

www.target.com/search.php?q=a&id=61278641278&msg=we+are+legion!

- Fixed target URL
 - + Carefully selected to create load on target server
- A Parameter with some arbitrary changing value
 - + To avoid caches along the way
- A Parameter value "msg" with some hacktivist's slogan
- HTTP Referer header – indicates attack code source



Anonymous and LOIC in Action



DDoS Is Moving Up the Stack

- Decreasing costs
 - + Application layer attacks are far more efficient
 - + Less attackers to take down a site
- The DoS security gap
 - + Traditionally, the defense against DDoS was based on dedicated devices operating at lower layers (TCP/IP).
 - Don't decrypt SSL
 - Don't understand the HTTP protocol
 - Unaware of the web application.

For more: <http://blog.imperva.com/2011/12/top-cyber-security-trends-for-2012-7.html>

32

iMPERVA®

DDoS Is Moving Up the Stack

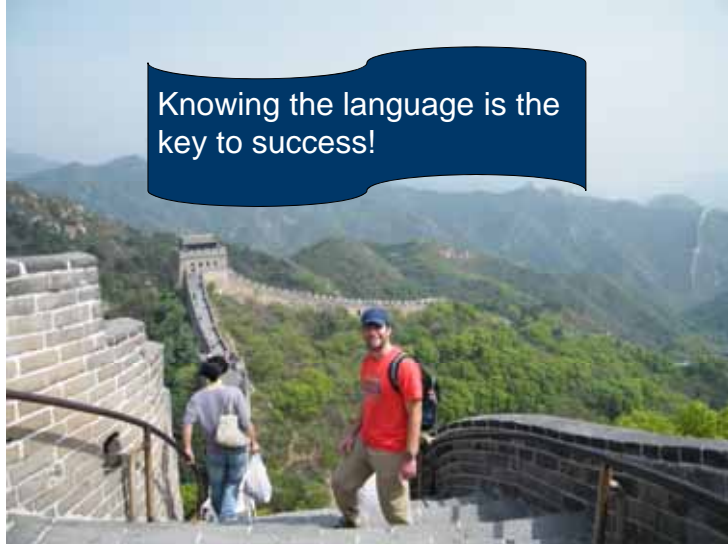


Mitigation

WAF: It can decrypt SSL, understand HTTP and also understand the application business logic to analyze the traffic, sifting out the DoS traffic.

我不會說中文

Knowing the language is the
key to success!



35

 **iMPERVA**

4

Non-Mitigations

 **iMPERVA**

Anti-Virus is Irrelevant: Malware is NOT the MO



McAfee mea culpa

"The security industry may need to reconsider some of its fundamental assumptions, including 'Are we really protecting users and companies?'"

--McAfee, September 2011

Source: <http://www.nytimes.com/internal/readersweb/2011/09/23/23readersweb-mcafee-to-security-industry-are-we-really-protecting-users-and-companies.html?partner=rps&emc=oss>

37



I have IPS and NGFW, am I safe?

- IPS and NGFWs do not prevent web application attacks.
 - + Don't confuse "application aware marketing" with Web Application Security.
- WAFs at a minimum must include the following to protect web applications:

- Web-App Profile
- Web-App Signatures
- Web-App Protocol Security
- Web-App DDOS Security
- Web-App Cookie Protection
- Anonymous Proxy/TOR IP Security
- HTTPS (SSL) visibility

Security Policy Correlation

38



I have IPS and NGFW, am I safe?

- IPS and NGFWs do not prevent web application attacks.
 - + Don't confuse "application aware marketing" with Web Application Security.
- However, **IPS and NGFWs** at best only partially support the items in **Red**:

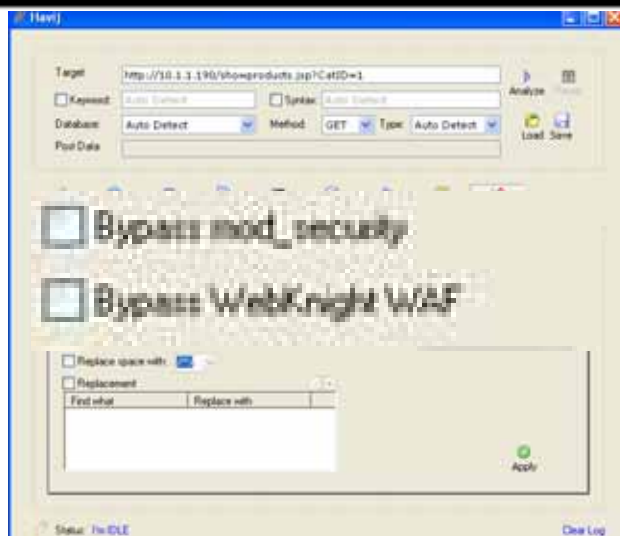
- Web-App Profile
- **Web-App Signatures**
- Web-App-Protocol-Security
- Web-App-DDOS-Security
- Web-App-Cookie-Protection
- Anonymous-Proxy/TOR-IP-Security
- **HTTPS (SSL) visibility**

Security Policy Correlation

39



WAF is the solution - Hackers realize it too



40



5

Mitigations



Automated Scanning Tools

The screenshot displays the IMPERVA SECURESPHERE interface. The top navigation bar includes links for Main, Admin, Preferences, Tasks, and Log out. Below this, a secondary bar contains Discovery & Classification, Setup, Profile, Risk Management, Policies, Audit, Reports, Monitor, and Threat Radar. The main content area is divided into several sections:

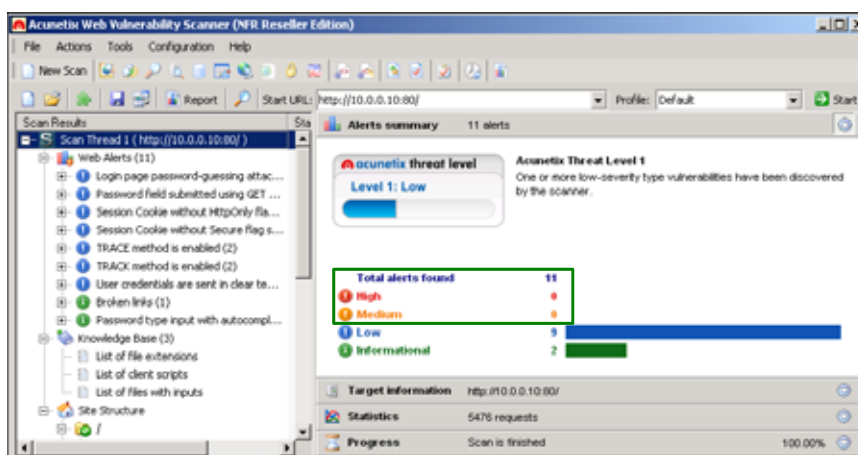
- Alerts (filtered):** A table listing alerts with columns for No., Updated, and Alert Description. The table shows a list of alerts, with the following details visible:

No.	Updated	Alert Description
2717	15:55:44	2237 Automated Vulnerability Scanning
2707	15:55:44	725 Suspicious Response Code
2706	15:55:44	9404 Multiple signatures from 10.0.0.1
2741	15:55:43	32 Multiple SQL injection from 10.0.0.1
2715	15:55:37	158 Multiple Cross-site scripting from 10.0.0.1
2724	15:55:37	156 Directory Traversal (In Cookies:Parameters Value)
2719	15:55:37	44 Multiple Illegal Byte Code Character in URL from 10.0.0.1
2718	15:55:37	21 Multiple NULL Character in Uri from 10.0.0.1
2709	15:55:37	319 Multiple signatures from 10.0.0.1
2721	15:55:35	73 Multiple Illegal HTTP Version from 10.0.0.1
2725	15:55:35	57 Multiple Redundant UTF-8 Encoding from 10.0.0.1
2722	15:55:35	63 Multiple Abnormally Long Request from 10.0.0.1
2727	15:55:35	60 Multiple NULL Character in Parameter Value from 10.0.0.1
2728	15:55:29	28 Multiple Double URL Encoding from 10.0.0.1
2714	15:55:19	4 Multiple Unknown HTTP Request Method from 10.0.0.1
2713	15:55:04	21 Multiple Unauthorized Method for Known URL from 10.0.0.1
2729	15:52:34	89 Parameter Type Violation what in 10.0.0.10/dosear
2740	15:52:25	38 Parameter Type Violation string in 10.0.0.10/dosear
2738	15:52:06	16 Parameter Type Violation ajaxradio in 10.0.0.10/dosear
2732	15:51:52	31 Multiple Illegal Byte Code Character in Header Name
2734	15:51:52	31 Multiple Illegal Response Code from 10.0.0.1
2733	15:51:52	31 Multiple Malformed HTTP Header Line from 10.0.0.1
2720	15:51:51	162 Parameter Type Violation mode in 10.0.0.10/login.js
2721	15:51:51	29 Parameter Type Violation password in 10.0.0.10/login.js
- Alert 2741: Multiple SQL injection from 10.0.0.1**: A detailed view of a specific alert, showing actions (Immediate Block (Simulation Mode)), policy (Web Correlation Policy), and aggregated information (Aggregated from 15:51:58 (0 hour(s), 4 minute(s)), 32 alerts (last updated 15:51:58)).
- Violations:** A table listing violations with columns for Host, Method, URL, Input Type, and Parameter. The table shows a list of violations, with the following details visible:

Host	Method	URL	Input Type	Parameter
10.0.0.10	POST	/admin/adminlogin.jsp	parameter	mode
10.0.0.10	POST	/admin/adminlogin.jsp	parameter	mode
10.0.0.10	POST	/admin/adminlogin.jsp	parameter	mode
10.0.0.10	POST	/admin/adminlogin.jsp	parameter	mode
10.0.0.10	POST	/register.jsp	parameter	Pass
10.0.0.10	POST	/register.jsp	parameter	Pass
10.0.0.10	POST	/register.jsp	parameter	Pass
10.0.0.10	POST	/register.jsp	parameter	Pass

The IMPERVA logo is visible in the bottom right corner of the interface.

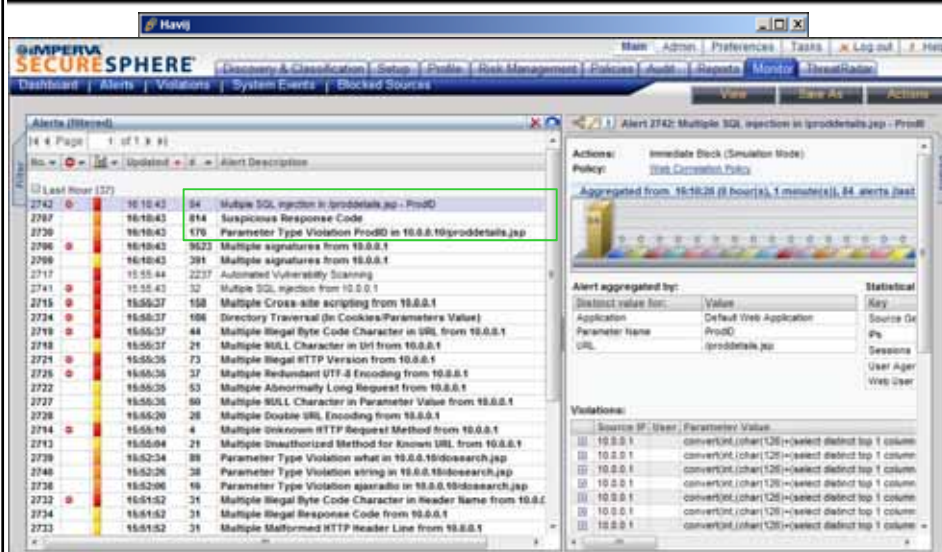
Automated Scanning Tools



43



Automated SQL Tool

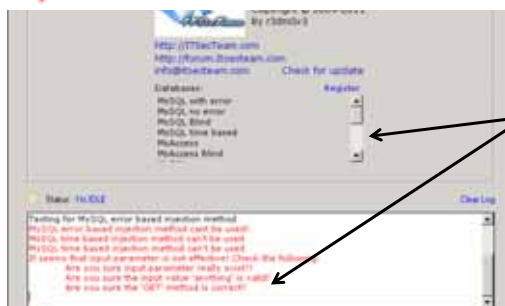


44



Automated SQL Tool

Testing for MySQL error based injection method
 MySQL error based injection method can't be used!
 MySQL time based injection method can't be used
 MySQL time based injection method can't be used
 It seems that input parameter is not effective! Check the following:
 Are you sure input parameter really exist?!
 Are you sure the input value 'anything' is valid?
 Are you sure the 'GET' method is correct?

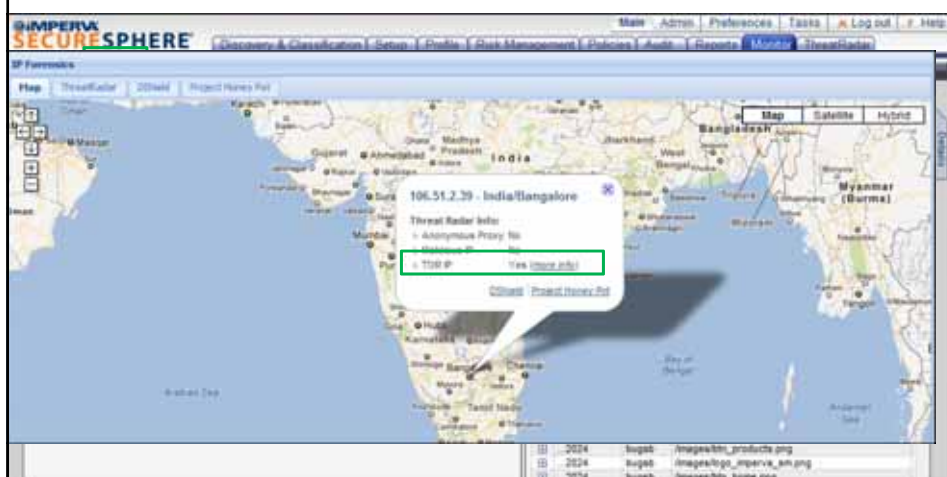


Havij SQL attack attempt fails with errors due to WAF mitigation.

45



Blocking Traffic Based on Reputation



46





Questions



Thank You